WHAT IS CLAIMED:

1. A method of accessing a password comprising:

dividing the password into a plurality of pieces;

storing pieces of the password on a different one of a plurality of servers, each of the plurality of servers being independent from others of the plurality of servers;

separately authenticating a user at each of the plurality of servers, each of the plurality of servers transmitting the piece of the password stored at the respective server to the user when the authentication at that server is successful; and

assembling the password from the password pieces transmitted from the plurality of servers.

2. The method of claim 1, wherein the password is a private key in a public/private key pair.

3. The method of claim 1, wherein a second password is used to authenticate the user at each of the plurality of servers, the second password being a weak password.

4. The method of claim 3, wherein each of the pieces of the password are encrypted before being stored on each of the servers, encryption keys for the encryption of the password pieces being derived from the second password.

5. The method of claim 1, wherein all but one of the pieces of the password are stored at the plurality of servers and one piece of the password is stored at a computer local to the user.

6. A method of securely storing a password comprising:

receiving an encrypted portion of the password, the encrypted portion of the password comprising less than the entire password;

storing the encrypted portion of the password with information identifying a user of the encrypted portion of the password;

receiving a request for the encrypted portion of the password, the request including the identification information; and

returning the encrypted portion of the password to the user when the identification information in the request matches the stored identification information.

7. The method of claim 6, wherein the password is a private key in a public/private key pair.

8. The method of claim 6, wherein the received encrypted portion of the password is encrypted based on a symmetric encryption of the portion of the password using a key based on a second password, the second password being a weak password.

9. The method of claim 8, wherein the information identifying the user of the encrypted portion of the password is based on the second password.

10. A method of receiving a first password of a user, the method comprising:

entering a second password of the user;

authenticating the user at each of a plurality of servers based on the second password, the plurality of servers being independent from one another;

receiving an encrypted version of a portion of the first password from each of the plurality of servers at which the authentication was successful, each of the portions of the first password containing less than the entire password;

decrypting the received encrypted portions of the first password using encryption keys based on the second password; and

assembling the first password from the decrypted portions.

11. The method of claim 10, wherein the first password is a strong user password.

12. The method of claim 10, wherein the first password is a private key in a public/private key pair.

13. The method of claim 10, wherein the second password is a weak password.

14. A method of authenticating a user at a remote computer system comprising:

transmitting each of portions of a password entered by the user and divided into a plurality of pieces to corresponding ones of a plurality of remote servers, each

of the plurality of remote servers being independent from others of the plurality of remote servers, and each of the servers having a respective piece of the password pre-registered with the server;

comparing the transmitted pieces of the password to the pre-registered versions of the password at the plurality of servers;

generating an authentication accept message at each of the plurality of servers at which the pre-registered version of the piece of the password matches the transmitted portions of the password; and

authenticating the user when the authentication accept message is generated for all of the pieces of the password at the plurality of servers.

15. The method of claim 14, wherein a piece of the password is pre-registered at a computer local to the user and the authentication accept message is generated by the computer local to the user when the pre-registered piece of the password at the computer local to the user matches a corresponding piece of the password entered by the user.

16. The method of claim 15, wherein the authentication accept messages are received and accepted at a content server remote from the user.

17. A computer server comprising:

a computer memory; and

a processor coupled to the computer memory, the processor receiving an encrypted portion of a password, the encrypted portion of the password comprising less than the entire password; storing the encrypted portion of the password with

information identifying a user of the encrypted portion of the password; receiving a request for the encrypted portion of the password, the request including the identification information; and returning the encrypted portion of the password to the user when the identification information in the request matches the stored identification information; wherein

the computer server is independent of other computer servers storing other portions of the password.

18. The computer server of claim 17, wherein the password is a private key in a public/private key pair.

19. The computer server of claim 17, wherein the received encrypted portion of the password is encrypted based on a symmetric encryption of the portion of the password using a key based on a second password, the second password being a weak password.

20. The computer server of claim 19, wherein the information identifying the user of the encrypted portion of the password is based on the second password.

21. A computer readable medium containing computer instructions that when executed by a processor cause the processor to perform operations for securely storing a password comprising:

receiving an encrypted portion of the password, the encrypted portion of the password comprising less than the entire password;

storing the encrypted portion of the password with information identifying a user of the encrypted portion of the password;

receiving a request for the encrypted portion of the password, the request including the identification information; and

returning the encrypted portion of the password to the user when the identification information in the request matches the stored identification information.

22. The computer readable medium of claim 21, wherein the password is a private key in a public/private key pair.

23. The computer readable medium of claim 21, wherein the received encrypted portion of the password is encrypted based on a symmetric encryption of the portion of the password using a key based on a second password, the second password being a weak password.

24. The computer readable medium of claim 23, wherein the information identifying the user of the encrypted portion of the password is based on the second password.

25. A computer readable medium containing computer instructions that when executed by a processor cause the processor to perform operations that receive a first password of a user, comprising:

receiving a second password entered by the user;

authenticating the user at each of a plurality of servers based on the second password, the plurality of servers being independent from one another;

receiving an encrypted version of a portion of the first password from each of the plurality of servers at which the authentication was successful, each of the portions of the first password containing less than the entire password;

decrypting the received encrypted portions of the first password using encryption keys based on the second password; and

assembling the first password from the decrypted portions.

26. The computer readable medium of claim 25, wherein the first password is a strong user password.

27. The computer readable medium of claim 25, wherein the first password is a private key in a public/private key pair.

28. The computer readable medium of claim 25, wherein the second password is a weak password.